CLAIMS

1. A digital rights management system for controlling the distribution of digital content to player applications, the system comprising:

a verification system to validate the integrity of the player applications;

a trusted content handler to decrypt content and to transmit the decrypted content to the player applications, using an extension mechanism defined by the application, and to enforce usage rights associated with the content; and

a user interface control module to ensure that users of the player applications are not exposed to actions that violate the usage rights;

wherein the digital rights management system operates independently without cooperation from the player applications.

2. A digital rights management system according to Claim 1, wherein the verification system includes an off-line verifier to verify that the player applications have certain properties, and to issue trust certificates to verify that the player applications have said properties.

3. A digital rights management system according to Claim 2, wherein the verification system further includes a verifying launcher for verifying that a particular player application is certified as a trusted application before digital content is transmitted to said particular player application.

4. A digital rights management system according to Claim 1, wherein the player applications request protected content, and the trusted content handler includes an authenticator to verify that a player application that

requests protected content has been authorized by the verification system to access the requested, protected content.

5. A digital rights management system according to Claim 1, wherein a user interface control module traps user interface related messages generated as a result of user interactions with player applications, blocks messages that lead to usage rights violations, and passes through other messages to the player applications.

6. A digital rights management method for controlling the distribution of digital content to player applications, the method comprising the steps:

providing a verification system to validate the integrity of the player applications;

using a trusted content handler to decrypt content and to transmit the decrypted content to the player applications, using an extension mechanism defined by the applications, and to enforce usage rights associated with the content; and

providing a user interface control module to ensure that users of the player applications are not exposed to actions that violate the usage rights;

wherein the digital rights management system operates independently without cooperation from the player applications.

7. A method according to Claim 6, wherein the step of providing a verification system includes the step of providing an off-line verifier to verify that the player applications have certain properties, and to issue trust certificates to verify that the player applications have said properties.

8. A method according to Claim 7, wherein the step of providing a verification system further includes the step of providing a verifying launcher for verifying that a particular player application is certified as a trusted application before digital content is transmitted to said particular player application.

9. A method according to Claim 6, wherein the player applications request protected content, and the step of using the trusted content handler includes the step of using an authenticator to verify that a player application that requests protected content has been authorized by the verification system to access the requested, protected content.

10. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method for controlling the distribution of digital content to player applications, the method steps comprising:

using a verification system to validate the integrity of the player applications;

using a trusted content handler to decrypt content and to transmit the decrypted content to the player applications, using an extension mechanism defined by the applications, and to enforce usage rights associated with the content; and

using a user interface control module to ensure that users of the player applications are not exposed to actions that violate the usage rights;

wherein said method operates independently without cooperation from the player applications.

11. A program storage device according to Claim 10, wherein the step of using the verification system includes

the step of using an off-line verifier to verify that the player applications have certain properties, and to issue trust certificates to verify that the player applications have said properties.

12. A program storage device according to Claim 11, wherein the step of using the verification system further includes the step of using a verifying launcher for verifying that a particular player application is certified as a trusted application before digital content is transmitted to said particular player application.

13. A program storage device according to Claim 10, wherein the player applications request protected content, and the step of using the trusted content handler includes the step of using an authenticator to verify that a player application that requests protected content has been authorized by the verification system to access the requested, protected content.

14. A code identity and integrity verification system, comprising:

a certificate generator for receiving applications, for determining if the applications exhibit a predefined property, and for issuing a trust certificate for each of the applications that exhibits the predefined property;

a certificate repository for receiving and storing trust certificates issued by the certificate generator;

a code verifier for verifying that a particular player application is certified as a trusted application before digital content is transmitted to said particular player application; and

an authenticator for receiving requests, using an extension mechanism defined by the applications, to verify that a player application that requests protected content has been authorized by the verification system to access the requested, protected content.

15. A code identify and integrity verification system according to Claim 14, wherein the code verifier is responsible for launching the player application and verifying the identity and integrity of the code using the information in the trust certificate before launching the application; the launch procedure returning process identification information, which the code verifier records internally; the authenticator communicating the same or other process identification information concerning its own process, which it obtains from system service calls, to the code verifier at the time the application requests content from the authenticator; the code verifier matching this process identification information against the process identification information it recorded; the code verifier returning a code indicating whether the process was verified or not.

16. A code identity and integrity verification system according to Claim 14, wherein the code verifier receives from the authenticator process identification information at the time the player application calls the authenticator; the code verifier querying the operating system with the process identification information or the file names of all modules loaded for that process; the code verifier using the information in the trust certificate to verify the identity and integrity of the code modules; returning a code indicating whether the process was verified or not.

17. A code identity and integrity verification system according to Claim 14, wherein the trust certificate includes:

a program identifier identifying said one of the applications;

a property name identifying an attribute certified by the trust certificate;

a code digest of the one application;

a digital signature containing a secret key of the application certifier; and

a certifier identification containing a public key of the application certifier.

18. A method for verifying the identity and integrity of code, comprising the steps:

using a certificate generator for receiving applications, for determining if the applications exhibit a predefined property, and for issuing a trust certificate for each of the applications that exhibits the predefined property;

receiving and storing in a certificate repository trust certificates issued by the certificate generator;

using a code verifier for verifying that a particular player application is certified as a trusted application before digital content is transmitted to said particular player application; and

using an authenticator for receiving requests, using an extension mechanism defined by the application, to verify that a player application that requests protected content has been authorized by the verification system to access the requested, protected content.

19. A method according to Claim 16, wherein the trust certificate includes:

a program identifier identifying said one of the applications;

a property name identifying an attribute certified by the trust certificate;

a code digest of the one application;

a digital signature containing a secret key of the application certifier; and

a certifier identification containing a public key of the application certifier.

20. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for verifying, out of process, the identity of code, said method steps comprising:

using a certificate generator for receiving applications, for determining if the applications exhibit a predefined property, and for issuing a trust certificate for each of the applications that exhibits the predefined property;

receiving and storing in a certificate repository trust certificates issued by the certificate generator;

using a code verifier for verifying that a particular player application is certified as a trusted application before digital content is transmitted to said particular player application; and

using an authenticator for receiving requests, using an extension mechanism defined by the application, to verify that a player application that requests protected content has been authorized by the verification system to access the requested, protected content.

21. A program storage device according to Claim 20, wherein the trust certificate includes:

a program identifier identifying said one of the applications;

a property name identifying an attribute certified by the trust certificate;

a code digest of the one application;

a digital signature containing a secret key of the application certifier; and

a certifier identification containing a public key of the application certifier.